

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/016450

International filing date: 07 September 2005 (07.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-298245
Filing date: 12 October 2004 (12.10.2004)

Date of receipt at the International Bureau: 13 October 2005 (13.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 1 0 月 1 2 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 2 9 8 2 4 5

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 2 9 8 2 4 5

出 願 人
Applicant(s): 日 本 電 信 電 話 株 式 会 社

2 0 0 5 年 9 月 2 8 日

特許庁長官
Commissioner,
Japan Patent Office.

中 嶋



【書類名】 特許願
【整理番号】 NTTH166072
【提出日】 平成16年10月12日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 12/56
H04L 12/46
【発明者】
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
【氏名】 三好 潤
【発明者】
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
【氏名】 長島 雅夫
【特許出願人】
【識別番号】 000004226
【氏名又は名称】 日本電信電話株式会社
【代理人】
【識別番号】 100089118
【弁理士】
【氏名又は名称】 酒井 宏明
【選任した代理人】
【識別番号】 100114306
【弁理士】
【氏名又は名称】 中辻 史郎
【手数料の表示】
【予納台帳番号】 036711
【納付金額】 16,000円
【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 0310351

【書類名】特許請求の範囲

【請求項1】

ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、

前記中継装置は、

前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手段と、

前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該ゲート装置に転送する転送手段とを備え、

前記ゲート装置は、

前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、

前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とするサービス不能攻撃防御システム。

【請求項2】

前記ゲート装置は、前記攻撃検知手段により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手段と、前記容疑シグネチャ生成手段により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手段とをさらに備え、前記転送手段は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする請求項1に記載のサービス不能攻撃防御システム。

【請求項3】

前記通過制御手段は、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴とする請求項2に記載のサービス不能攻撃防御システム。

【請求項4】

前記ゲート装置は、前記容疑シグネチャ生成手段により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手段をさらに備え、前記パケット制限手段は、前記容疑シグネチャ生成手段により生成された容疑シグネチャおよび前記正規シグネチャ生成手段により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項3に記載のサービス不能攻撃防御システム。

【請求項5】

前記ゲート装置は、前記正規シグネチャ生成手段により生成された正規シグネチャを前記中継装置に転送するシグネチャ転送手段をさらに備えたことを特徴とする請求項4に記載のサービス不能攻撃防御システム。

【請求項6】

ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、

前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納工程と、

前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情

報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送工程と、

前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御工程とを含んだことを特徴とするサービス不能攻撃防御方法。

【請求項 7】

前記ゲート装置が前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得工程とをさらに含み、前記転送工程は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする請求項 6 に記載のサービス不能攻撃防御方法。

【請求項 8】

前記通過制御工程は、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする請求項 7 に記載のサービス不能攻撃防御方法。

【請求項 9】

前記ゲート装置が前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程をさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項 8 に記載のサービス不能攻撃防御方法。

【請求項 10】

ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、

前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納手順と、

前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送手順と、

前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手順と

を含んだことを特徴とするサービス不能攻撃防御プログラム。

【請求項 11】

前記ゲート装置が前記攻撃検知手順により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手順と、前記容疑シグネチャ生成手順により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手順とをさらに含み、前記転送手順は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする請求項 10 に記載のサービス不能攻撃防御プログラム。

【請求項 12】

前記通過制御手順は、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順

と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とを含んだことを特徴とする請求項 1 1 に記載のサービス不能攻撃防御プログラム。

【請求項 1 3】

前記ゲート装置が前記容疑シグネチャ生成手順により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手順をさらに含み、前記パケット制限手順は、前記容疑シグネチャ生成手順により生成された容疑シグネチャおよび前記正規シグネチャ生成手順により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項 1 2 に記載のサービス不能攻撃防御プログラム。

【書類名】明細書

【発明の名称】サービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラム

【技術分野】

【0001】

この発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくはこの中継装置で通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関し、特に、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関する。

【背景技術】

【0002】

従来、ネットワークを介した攻撃としてサービス不能攻撃および分散型サービス不能攻撃（Distributed Denial of Service Attack、以下単に「DDoS攻撃」と言う）が知られている。かかるDDoS攻撃から通信機器を防御する分散型サービス不能攻撃防御システムでは、攻撃対象となる通信機器とネットワークとの間に設けられたゲートウェイ装置やネットワークを構成するルータ装置がパケットを制限することになる。具体的には、ネットワークを介して通信機器に向けて送信されたパケットを正規パケット、容疑パケットまたは不正パケットに分類し、通信機器に送信されるパケットを制限していた（例えば、特許文献1参照）。

【0003】

このような従来の分散型サービス不能攻撃防御システムにおいては、あらかじめ登録された攻撃検知条件に基づいてゲートウェイ装置が攻撃を検知すると、攻撃検知されたパケットの特徴を示す容疑シグネチャが生成され、生成された容疑シグネチャがネットワークを構成するルータ装置等の中継装置に転送される。

【0004】

一方、容疑シグネチャに当てはまるパケットのうち通信機器に対する攻撃とみなされないパケット（以下「非攻撃パケット」と言う）の特徴を表す正規シグネチャが、あらかじめ登録された正規条件情報に基づいてゲートウェイ装置によって生成され、生成された正規シグネチャがネットワークを構成するルータ装置等の中継装置に転送される。

【0005】

容疑シグネチャおよび正規シグネチャが転送された中継装置並びにゲートウェイ装置によって中継されるパケットは、容疑シグネチャおよび正規シグネチャに基づいてシェーピングやフィルタリング等の処理が施される。

【0006】

このように、従来の分散型サービス不能攻撃防御システムは、攻撃を行うパケットの通過を出来るだけ攻撃元の近くで制限することによって、攻撃を行うパケット（以下「攻撃パケット」と言う）による悪影響を出来るだけ小さくするようになっている。

【0007】

【特許文献1】特開2003-283554号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、従来の分散型サービス不能攻撃防御システムにおいては、攻撃から防御する対象の通信機器に対する非攻撃パケットの条件を表す正規条件情報の追加や変更等の管理がゲートウェイ装置のオペレータによって行われるため、正規条件情報の管理が煩雑になるといった課題があった。

【0009】

本発明は、上述した従来技術による問題点を解消するためになされたものであり、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御方法、サービス不能攻撃防御装置およびサービス不能攻撃防御プログラムを提供することを目的とする。

【課題を解決するための手段】

【0010】

上述した課題を解決し、目的を達成するため、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、前記中継装置は、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手段と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該ゲート装置に転送する転送手段とを備え、前記ゲート装置は、前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とする。

【0011】

この発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【0012】

また、本発明は、上記発明において、前記ゲート装置は、前記攻撃検知手段により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手段と、前記容疑シグネチャ生成手段により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手段とをさらに備え、前記転送手段は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする。

【0013】

この発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【0014】

また、本発明は、上記発明において、前記通過制御手段は、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴とする。

【0015】

この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

【0016】

また、本発明は、上記発明において、前記ゲート装置は、前記容疑シグネチャ生成手段により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手段をさらに備え、前記パケット制限手段は、前記容疑シグネチャ生成手段により生成された容疑シグネチャおよび前記正規シグネチャ生成手段により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。

【0017】

この発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。

【0018】

また、本発明は、上記発明において、前記ゲート装置は、前記正規シグネチャ生成手段により生成された正規シグネチャを前記中継装置に転送するシグネチャ転送手段をさらに備えたことを特徴とする。

【0019】

この発明によれば、ゲート装置が生成された正規シグネチャを中継装置に転送することとしたので、ゲート装置のみならず中継装置においても効率良くパケットの通過制御をおこなうことができる。

【0020】

また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納工程と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送工程と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御工程とを含んだことを特徴とする。

【0021】

この発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【0022】

また、本発明は、上記発明において、前記ゲート装置が前記攻撃検知工程により攻撃が

検知されたバケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得工程とをさらに含み、前記転送工程は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする。

【0023】

この発明によれば、ゲート装置は、攻撃が検知されたバケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【0024】

また、本発明は、上記発明において、前記通過制御工程は、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて非攻撃バケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ネットワークから受信したバケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するバケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうバケットの通過を制限するバケット制限工程とを含んだことを特徴とする。

【0025】

この発明によれば、取得された正規アドレス情報に基づいて非攻撃バケットの条件を示す正規条件情報を生成し、ネットワークから受信したバケットのうち正規条件情報に示された条件に適合するバケットの通過を許容しつつ、通信機器へ攻撃をおこなうバケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なバケットの通過制御をおこなうことができる。

【0026】

また、本発明は、上記発明において、前記ゲート装置が前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するバケットのうち、前記正規条件情報に示された条件に適合するバケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程をさらに含み、前記バケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したバケットの通過を制限することを特徴とする。

【0027】

この発明によれば、ゲート装置が容疑シグネチャに該当するバケットのうち、正規条件情報に示された条件に適合するバケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したバケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くバケットの通過制御をおこなうことができる。

【0028】

また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃バケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納手順と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送手順と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃バケットの条件を示す正規条件情報に基づいてバケットの通過制御をおこなう通過制御手順とを含んだことを特徴とする。

【0029】

この発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【0030】

また、本発明は、上記発明において、前記ゲート装置が前記攻撃検知手順により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手順と、前記容疑シグネチャ生成手順により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手順とをさらに含み、前記転送手順は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする。

【0031】

この発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【0032】

また、本発明は、上記発明において、前記通過制御手順は、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とを含んだことを特徴とする。

【0033】

この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

【0034】

また、本発明は、上記発明において、前記ゲート装置が前記容疑シグネチャ生成手順により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手順をさらに含み、前記パケット制限手順は、前記容疑シグネチャ生成手順により生成された容疑シグネチャおよび前記正規シグネチャ生成手順により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。

【0035】

この発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという指標を用い

て効率良くパケットの通過制御をおこなうことができる。

【発明の効果】

【0036】

本発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうよう構成したので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【0037】

また、本発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得するよう構成したので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【0038】

また、本発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するよう構成したので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

【0039】

また、本発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限するよう構成したので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。

【0040】

また、本発明によれば、ゲート装置が生成された正規シグネチャを中継装置に転送するよう構成したので、ゲート装置のみならず中継装置においても効率良くパケットの通過制御をおこなうことができる。

【発明を実施するための最良の形態】

【0041】

以下に添付図面を参照して、この発明に係るサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムの好適な実施の形態を詳細に説明する。

【実施例】

【0042】

図1は、本実施例に係る分散型サービス不能攻撃防御システム1の構成を示すブロック図である。同図に示す分散型サービス不能攻撃防御システム1は、通信機器7への分散型サービス不能攻撃を主としてゲート装置8で防御するシステムである。具体的には、ネットワーク2上に所在する正当な装置（アドレス発行サーバ10）により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置8が取得し、取得した正規アドレス情報に基づいてゲート装置8が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケット

の通過を許容しつつ、通信機器 7 へ攻撃をおこなうパケットの通過を制限するようにしている。なお、このゲート装置 8 が正規条件情報に基づいて生成した正規シグネチャ並びに容疑シグネチャは中継装置 6 などに転送され、中継装置でのフィルタリングを可能ならしめている。

【0043】

従来、かかる正規アドレス情報の追加や変更等の管理は、ゲート装置 8 のオペレータによって行われていたため、正規条件情報の管理が煩雑になるという問題があった。このため、本実施例では、かかる正規アドレス情報の追加をゲート装置 8 のオペレータに担わせるのではなく、アドレス発行サーバ 10 などの正当な端末から正規アドレス情報を取得することとしている。このため、本実施例によれば、ゲート装置 8 のオペレータの管理負担を軽減することができる。

【0044】

ここで、このゲート装置 8 が正規アドレス情報を取得する際に、本実施例では、アドレス発行サーバ 10 が中継装置 6 に対して正規アドレス情報を送信し（図 1 のステップ 1）、この中継装置 6 に正規アドレス情報を記憶させ（図 1 のステップ 2）、ゲート装置 8 が攻撃を検知したパケットの特徴を表す容疑シグネチャを生成して生成した容疑シグネチャを中継装置 6 に送信すると（図 1 のステップ 3）、あらかじめ記憶した正規アドレス情報をゲート装置 8 に転送し（図 1 のステップ 4）、ゲート装置 8 が正規アドレス情報に基づいて正規条件情報を自動生成する（図 1 のステップ 5）こととしている。

【0045】

次に、この分散型サービス不能攻撃防御システム 1 のシステム構成について説明する。図 1 に示すように、この分散型サービス不能攻撃防御システム 1 は、ネットワーク 2 を介して伝送されるパケットを中継する複数の中継装置 3～6 と、ネットワーク 2 を介して通信機器 7 に送信されるパケットの通過を制限するゲート装置 8 とを備えている。なお、図 1 に示した分散型サービス不能攻撃防御システム 1 の構成は一例を示すものであり、中継装置およびゲート装置等の数量やネットワーク構成を限定するものではない。

【0046】

ゲート装置 8 は、ネットワーク間接続機器であるゲートウェイ装置などによって構成され、コンピュータ装置等によって構成される通信機器 7 を含む構内情報通信網（Local Area Network、以下単に「LAN」と記載する。）14 に接続されている。また、中継装置 3～6 は、ルータ装置によってそれぞれ構成されている。なお、この中継装置 3～6 は、ブリッジによって構成することもできる。

【0047】

ここで、中継装置 3 は、中継装置 4 およびゲート装置 8 に接続され、中継装置 4 は、通信機器 15 および中継装置 3 に接続され、中継装置 5 は、通信機器 16 および中継装置 6 に接続され、中継装置 6 は、中継装置 5、エッジルータ 11 およびゲート装置 8 に接続されている。

【0048】

図 2 は、図 1 に示したゲート装置 8 の構成を示すブロック図である。図 2 に示すように、このゲート装置 8 は、ネットワーク 2 から受信されたパケットによる攻撃を検知する攻撃検知部 20 と、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成部 21 と、通信機器 7 に対する攻撃とみなされないパケット（非攻撃パケット）の条件を表す正規条件情報を格納する正規条件情報格納部 22 と、正規条件情報格納部 22 に格納される正規条件情報を生成する正規条件情報生成部 23 と、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成部 24 と、容疑シグネチャに当てはまるパケットのうち、通信機器 7 に対する攻撃とみなすパケットの特徴を表す不正シグネチャを生成する不正シグネチャ生成部 25 と、容疑シグネチャ、正規シグネチャおよび不正シグネチャに基づいてネットワーク 2 から受信されたパケットの通過を制限するパケット制限部 26 と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置 3 および中

継装置 6 に転送するシグネチャ転送部 27 と、ネットワーク 2 に接続された各装置と通信を行うネットワークインタフェース 28 とを備えている。

【0049】

攻撃検知部 20 は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図 3 は、攻撃検知条件の一例を示す図である。図 3 において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる 3 組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。

【0050】

例えば、1 番目の検知条件は、宛先のアドレス情報が 192.168.1.1 であり (Dst=192.168.1.1/32)、トランスポート層のプロトコルが TCP (Transmission Control Protocol) であり (Protocol=TCP)、TCP ポート番号が 80 である (Port=80) パケットが検知対象となり、この検知対象のパケットの伝送レートが 500 kbps を超えた状態が 10 秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0051】

同様に、2 番目の検知条件は、宛先のアドレス情報が 192.168.1.2 であり (Dst=192.168.1.2/32)、トランスポート層のプロトコルが UDP (User datagram protocol) である (Protocol=UDP) パケットが検知対象となり、この検知対象のパケットの伝送レートが 300 kbps を超えた状態が 10 秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0052】

また、3 番目の検知条件は、宛先のアドレス情報が 192.168.1.0~192.168.1.255 の範囲内である (Dst=192.168.1.0/24) パケットが検知対象となり、この検知対象のパケットの伝送レートが 1 Mbps を超えた状態が 20 秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【0053】

このように、検知対象のパケットによる攻撃が攻撃検知部 20 によって検知されると、容疑シグネチャ生成部 21 は、検知対象のパケットの特徴を表す容疑シグネチャを生成する。例えば、図 3 における攻撃検知条件の 1 番目の検知条件に合う攻撃が検知された場合には、容疑シグネチャ生成部 21 は、宛先のアドレス情報が 192.168.1.1 であり、トランスポート層のプロトコルが TCP であり、TCP ポート番号が 80 であるパケットを示す容疑シグネチャを生成する。なお、容疑シグネチャは、対象となるパケットに対するシェーピングやフィルタリング等の処理や、この処理に関するパラメータ等を含むようにしてもよい。

【0054】

正規条件情報格納部 22 は、フラッシュメモリなどの不揮発性の記憶媒体によって構成されている。図 4 は、正規条件情報格納部 22 に格納される正規条件情報の一例を示す図である。図 4 において、正規条件情報は攻撃とみなされない条件である正規条件で構成される。

【0055】

例えば、1 番目の正規条件によって、送信元のアドレス情報が 172.16.10.0~172.16.10.255 の範囲内である (Src=172.16.10.0/24) パケットは、攻撃とみなされない。同様に、2 番目の正規条件によって、サービスタイプ (Type of Service) が 0x01 である (TOS=0x01) パケットは、攻撃とみなされない。

【0056】

正規条件情報生成部 23 は、本実施例の最も重要な特徴部分をなす処理部であり、オペレータの処理行為を伴うことなく正規条件情報格納部 22 に格納された正規条件情報の自動更新をおこなう。従来、かかる正規条件情報の管理はオペレータに委ねられていたが、本実施例では、かかる正規条件情報を自動更新している。

【0057】

具体的には、この正規条件情報生成部23は、ネットワーク2を介した攻撃を行わないパケットの送信元を表す正規アドレス情報が隣接する中継装置3または6から送信され、送信された正規アドレス情報がネットワークインタフェース28に受信された場合に、この正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以って正規条件情報格納部22に格納された正規条件情報を更新する。すなわち、正規アドレス情報を送信アドレスとしたパケットは、通信機器7に対する攻撃とみなされないものとなる。なお、ここでは正規条件情報の追加を自動的におこなう点を強調したが、正規条件情報格納部22に格納された正規条件情報は、ゲート装置8のオペレータによって追加、削除、変更などの編集ができるようにしてもよい。

【0058】

正規シグネチャ生成部24は、容疑シグネチャ生成部21によって生成された容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する処理部である。

【0059】

例えば、この正規シグネチャ生成部24は、攻撃検知部20によって図3に示した1番目の攻撃検知条件に合う攻撃が検知された場合には、図4に示した正規条件情報に基づいて、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、送信元のアドレス情報が172.16.10.0~172.16.10.255の範囲内であるパケットを示す正規シグネチャと、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがTCPであり、TCPポート番号が80であり、サービスタイプが0x01であるパケットを示す正規シグネチャとを生成する。

【0060】

不正シグネチャ生成部25は、容疑シグネチャ生成部21によって生成された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャを生成する処理部である。

【0061】

図5は、不正条件の一例を示す図である。図5において、1番目の不正条件は、500kbps以上の伝送レートで30秒以上連続送信されているパケットを示している。同様に、2番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されているICMP (Internet Control Message Protocol) に準拠したエコー応答 (Echo Reply) パケットを示し、3番目の不正条件は、300kbps以上の伝送レートで15秒以上連続送信されている分割送信されたフラグメントパケットを示している。

【0062】

パケット制限部26は、容疑シグネチャ生成部21によって生成された容疑シグネチャと正規シグネチャ生成部24によって生成された正規シグネチャと不正シグネチャ生成部25によって生成された不正シグネチャに基づいてネットワークインタフェース28によって受信されたパケットの通過を制限するようになっている。

【0063】

具体的には、パケット制限部26は、不正シグネチャに当てはまるパケットを廃棄し、正規シグネチャに当てはまるパケットに対しては制限を加えずに通過させ、容疑シグネチャに当てはまるパケットに対しては容疑シグネチャに示された処理等に基づいて伝送帯域を絞った経路を介して通過させるようになっている。

【0064】

シグネチャ転送部27は、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置3および中継装置6に転送する処理部であり、中継装置3および中継装置6は、さらに隣接関係にある中継装置にパケットを転送する。なお、隣接関係とは、本発明に係るゲート装置および中継装置における隣接関係であり、物理的な接続関係とは異なる。

【0065】

図6は、図1に示した中継装置6の構成を示す機能ブロック図である。なお、ここでは

説明の便宜上中継装置 6 の構成を説明するが、他の中継装置 3 ～ 5 についても中継装置 6 と同様に構成されている。この中継装置 6 は、入力ポート 3 0 と、パケットをルーティングするためのスイッチ 3 1 と、出力ポート 3 2 と、不正シグネチャを生成する不正シグネチャ生成部 3 5 と、不正シグネチャならびにゲート装置 8 によって転送された容疑シグネチャおよび正規シグネチャに基づいて入力ポート 3 0 に入力されたパケットの通過を制限するパケット制限部 3 6 と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置 5 に転送するシグネチャ転送部 3 7 と、中継装置 6 の保持する正規アドレス情報を格納する正規アドレス情報格納部 3 8 と、正規アドレス情報格納部 3 8 に格納された正規アドレス情報を送信する正規アドレス情報送信部 3 9 を備えている。

【 0 0 6 6 】

ここで、不正シグネチャ生成部 3 5、パケット制限部 3 6 およびシグネチャ転送部 3 7 は、ゲート装置 8 を構成する不正シグネチャ生成部 2 5、パケット制限部 2 6 およびシグネチャ転送部 2 7 とそれぞれ同様に構成されるため、詳細な説明は省略する。なお、中継装置 6 は、ゲート装置 8 と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部および正規シグネチャ生成部を備えるようにしてもよい。

【 0 0 6 7 】

シグネチャ転送部 3 7 は、パケット制限部 3 6 によってパケットの通過が制限された後、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート 3 0 に受信されているか否かを判断し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート 3 0 に受信されていると判断した場合には、容疑シグネチャおよび正規シグネチャを転送し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート 3 0 に受信されていると判断しなかった場合には、容疑シグネチャおよび正規シグネチャを転送しない。

【 0 0 6 8 】

また、図 1 に示した構成においては、中継装置 4 および中継装置 5 には、容疑シグネチャおよび正規シグネチャを転送する中継装置が存在しないため、シグネチャ転送部 3 7 による容疑シグネチャおよび正規シグネチャの転送は行われない。

【 0 0 6 9 】

このように、ゲート装置 8 によって攻撃が検知された場合には、容疑シグネチャおよび正規シグネチャが生成され、生成された容疑シグネチャおよび正規シグネチャが各中継装置 3 ～ 6 に転送され、ゲート装置 8 および中継装置 3 ～ 6 においてパケットのシェーピングやフィルタリング等の処理が施される。このため、分散型サービス不能攻撃防御システム 1 においては、例えば、ゲート装置 8 によって検知された攻撃が通信機器 1 5 を介して行われている場合には、攻撃を行うパケットの通過が攻撃元の近く、すなわち中継装置 4 で制限され、攻撃を行うパケットによる悪影響が小さくなる。

【 0 0 7 0 】

アドレス情報格納部 3 8 は、不揮発性の記憶媒体によって構成されており、正規アドレス情報を保持する。

【 0 0 7 1 】

図 1 において、LAN 9 は、エッジルータ 1 1 を介してネットワーク 2 と接続されるとともに、コンピュータ装置等の通信機器 1 2、1 3 が接続されている。ここで、LAN 9 では、ネットワーク 2 を介した攻撃を行わないものとする。

【 0 0 7 2 】

LAN 9 に接続されたアドレス発行サーバ 1 0 は、LAN 9 のアドレス情報または LAN 9 に接続された通信機器 1 2、1 3 のアドレス情報を含む正規アドレス情報を中継装置 6 に向けて送信する。なお、このアドレス発行サーバ 1 0 は、正規アドレス情報を定期的に送信するようにしてもよく、アドレス発行サーバ 1 0 のオペレータによる起動に応じて送信するようにしてもよい。また、正規アドレス情報を送信するものとしては、アドレス発行サーバ 1 0 の他にエッジルータ 1 1 等の LAN 9 を構成する装置であれば何れのものでもよい。

【0073】

図6において、正規アドレス情報格納部38はさらに、アドレス発行サーバ10によって送信された正規アドレス情報を正規アドレス情報格納部38に追加するようになっている。

【0074】

以上のように構成された分散型サービス不能攻撃防御システム1について、図7～図10を用いてその動作を説明する。図7は、図1に示したゲート装置8の攻撃検知動作を示すフローチャートである。

【0075】

まず、攻撃検知条件に基づいてネットワークインタフェース28によって受信されたパケットによる攻撃が攻撃検知部20によって検知されると（ステップS1）、攻撃が検知されたパケットの特徴を表す容疑シグネチャが容疑シグネチャ生成部21によって生成される（ステップS2）。

【0076】

次に、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャが正規シグネチャ生成部24によって生成されるとともに（ステップS3）、容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部25によって生成される（ステップS4）。

【0077】

次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部26によるパケット通過条件として設定される（ステップS5）。また、容疑シグネチャおよび正規シグネチャがシグネチャ転送部27によって隣接関係にある中継装置3および中継装置6に転送される（ステップS6）。

【0078】

図8は、図1に示した中継装置6のシグネチャ受信動作を示すフローチャートである。まず、入力ポート30に容疑シグネチャおよび正規シグネチャが受信されると（ステップS10）、受信された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部35によって生成される（ステップS11）。

【0079】

次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部36によるパケット通過条件として設定される（ステップS12）。また、容疑シグネチャおよび正規シグネチャがシグネチャ転送部37によって隣接関係にある中継装置5に転送される（ステップS13）。さらに正規アドレス情報格納部38に保持している正規アドレス情報を容疑シグネチャの送信元であるゲート装置8に送信する（ステップS14）。

【0080】

図9は、図1に示したゲート装置8のパケット制限動作を示すフローチャートである。まず、ネットワークインタフェース28にパケットが受信されると（ステップS20）、受信されたパケットが不正シグネチャに当てはまるか否かがパケット制限部26によって判断される（ステップS21）。

【0081】

パケットが不正シグネチャに当てはまると判断された場合には、パケットがパケット制限部26によって廃棄される（ステップS22）、一方、パケットが不正シグネチャに当てはまらないと判断された場合には、パケットが正規シグネチャに当てはまるか否かがパケット制限部26によって判断される（ステップS23）。

【0082】

パケットが正規シグネチャに当てはまると判断された場合には、パケットの通過がパケット制限部26によって許可される（ステップS24）。一方、パケットが正規シグネチャに当てはまらないと判断された場合には、パケットが容疑シグネチャに当てはまるか否

かがバケット制限部26によって判断される（ステップS25）。

【0083】

バケットが容疑シグネチャに当てはまると判断された場合には、容疑シグネチャに示された処理等に基づいて伝送帯域が絞られた経路を介したバケットの通過が許可される（ステップS26）。一方、バケットが容疑シグネチャに当てはまらなと判断された場合には、バケットの通過がバケット制限部26によって許可される（ステップS24）。なお、中継装置3～6のバケット制限動作は、ゲート装置8のバケット制限動作と同様であるため説明を省略する。

【0084】

図10は、分散型サービス不能攻撃防御システム1の正規条件情報更新動作を示すシーケンス図である。まず、LAN9のアドレス発行サーバ10からLAN9内の正規アドレス情報が中継装置6に送信され（ステップS30）、中継装置6の正規アドレス情報格納部38に格納されるとともに（ステップS31）、通信装置16からの正規アドレス情報が中継装置5に送信され（ステップS32）、中継装置5の正規アドレス情報格納部38に格納される（ステップS33）。

【0085】

ここでゲート装置8において攻撃を検知すると（ステップS34）、対応する容疑シグネチャが生成され（ステップS35）、隣接する中継装置3および中継装置6に転送される（ステップS36）。以下では、簡単のため中継装置3および中継装置4へのシグネチャの転送については記述を省略する。

【0086】

中継装置6はゲート装置8から容疑シグネチャを受信すると、正規アドレス情報格納部38に格納してある正規アドレス情報をゲート装置8に送り返し（ステップS37）、容疑シグネチャをさらに中継装置5に転送する（ステップS41）。ここで、ステップS37とステップS41は順序を逆にすることが可能である。

【0087】

正規アドレス情報がゲート装置8のネットワークインタフェース28に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部23によって生成され、生成された正規条件情報を以って正規条件情報格納部22に格納された正規条件情報が更新される（ステップS38）。次いで、正規シグネチャ生成部24にて、対応する正規シグネチャが生成され、バケット制限と中継装置6への転送が行なわれる（ステップS39～S40）。

【0088】

一方、中継装置5は、中継装置6から容疑シグネチャを受信すると、正規アドレス情報格納部38に格納してある正規アドレス情報を容疑シグネチャの送信元である中継装置、すなわち中継装置6に送信する（ステップS42）。中継装置6は、中継装置5から受信した正規アドレス情報をそのままゲート装置8に送信する（ステップS43）。

【0089】

正規アドレス情報がゲート装置8のネットワークインタフェース28に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部23によって生成され、生成された正規条件情報を以って正規条件情報格納部22に格納された正規条件情報が更新される（ステップS44）。次いで、正規シグネチャ生成部24にて、対応する正規シグネチャが生成され、バケット制限と中継装置6への転送が行なわれる（ステップS45～S46）。

【0090】

以上説明したように、分散型サービス不能攻撃防御システム1によれば、ネットワーク2を介した攻撃を行わないバケットの送信元を表す正規アドレス情報がゲート装置8に送信され、ゲート装置8に送信された正規アドレス情報に基づいて、通信機器7に対する攻撃とみなされないバケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。

【0091】

なお、上記実施例に示したゲート装置8は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、コンピュータのROM(Read Only Memory)等に容疑シグネチャを送信して正規アドレス情報を取得するルーチン、正規アドレス情報に基づいて非攻撃バケットの条件を示す正規条件情報を生成するルーチン、ネットワークから受信したバケットのうち正規条件情報に示された条件に適合するバケットの通過を許容しつつ、通信機器へ攻撃をおこなうバケットの通過を制限するルーチンを含むプログラムを記憶しておき、かかるプログラムをCPUにロードして実行することにより、本発明に係るゲート装置8を形成することができる。

【産業上の利用可能性】

【0092】

以上のように、本発明にかかるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムは、サービス不能攻撃および分散型サービス不能攻撃から通信機器を防御する場合に適している。

【図面の簡単な説明】

【0093】

【図1】本実施例に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

【図2】図1に示したゲート装置の構成を示すブロック図である。

【図3】本実施例に係る攻撃検知条件の一例を示す図である。

【図4】本実施例に係る正規条件情報の一例を示す図である。

【図5】本実施例に係る不正条件の一例を示す図である。

【図6】図1に示した中継装置の構成を示すブロック図である。

【図7】図2に示したゲート装置の攻撃検知動作を示すフローチャートである。

【図8】図6に示した中継装置のシグネチャ受信動作を示すフローチャートである。

【図9】図2に示したゲート装置のバケット制限動作を示すフローチャートである。

【図10】本実施例に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

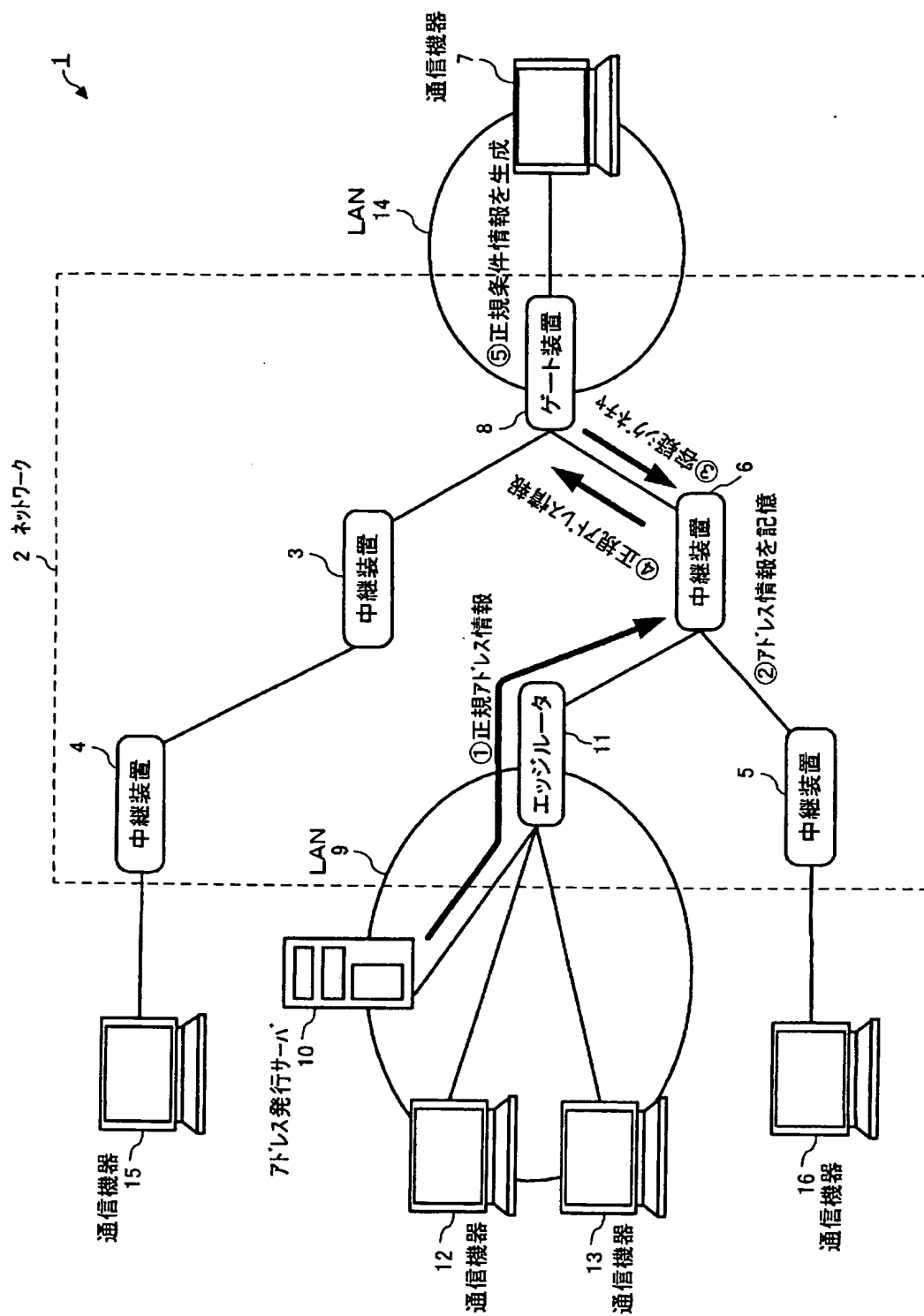
【符号の説明】

【0094】

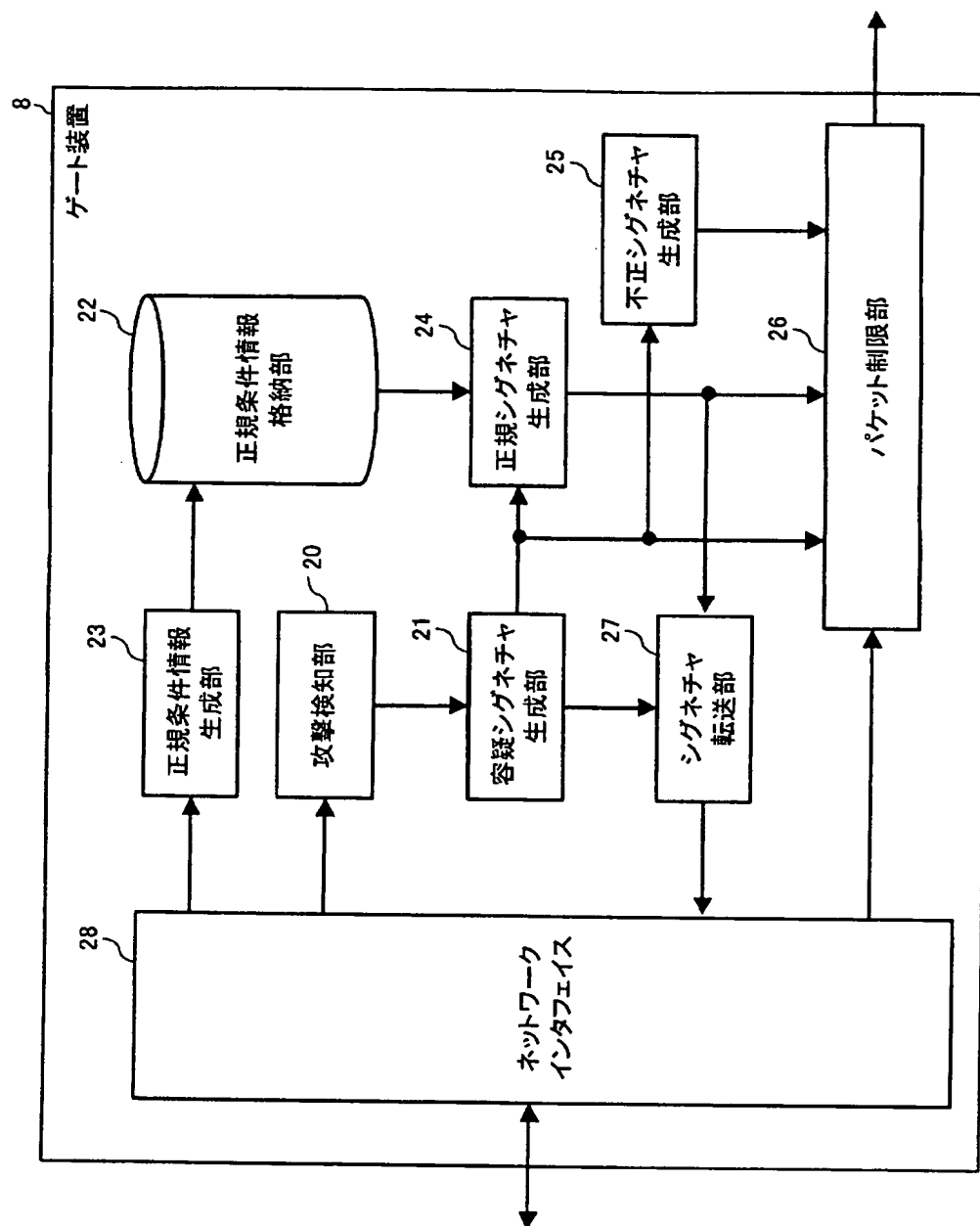
- 1 分散型サービス不能攻撃防御システム
- 2 ネットワーク
- 3、4、5、6 中継装置
- 7 通信機器
- 8 ゲート装置
- 9 LAN
- 10 アドレス発行サーバ
- 11 エッジルータ
- 12、13、15、16 通信機器
- 14 LAN
- 20 攻撃検知部
- 21 容疑シグネチャ生成部
- 22 正規条件情報格納部
- 23 正規条件情報生成部
- 24 正規シグネチャ生成部
- 25、35 不正シグネチャ生成部
- 26、36 バケット制限部
- 27、37 シグネチャ転送部
- 28 ネットワークインタフェース
- 30 入力ポート

- 3 1 スイッチ
- 3 2 出力ポート
- 3 8 アドレス情報記憶部
- 3 9 正規アドレス情報送信部

【書類名】 図面
【図 1】



【図2】



【図 3】

	検知属性	検知閾値	検出時間
1	[Dst=192.168.1.1/32, Protocol=TCP, Port=80]	500kbps	10秒
2	[Dst=192.168.1.2/32, Protocol=UDP]	300kbps	10秒
3	[Dst=192.168.1.0/24]	1Mbps	20秒

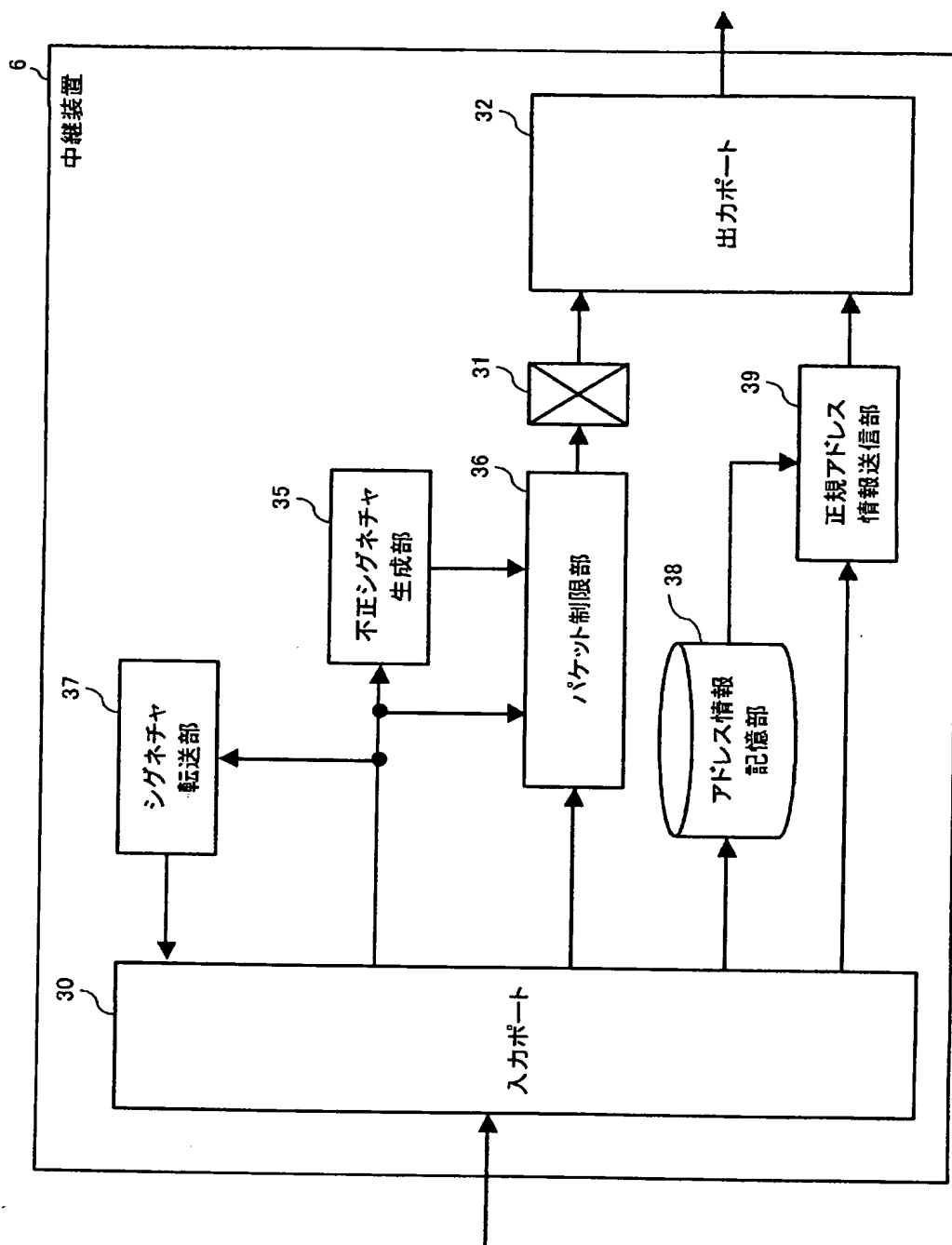
【図 4】

	正規条件
1	[Src=172.16.10.0/24]
2	[TOS=0x01]

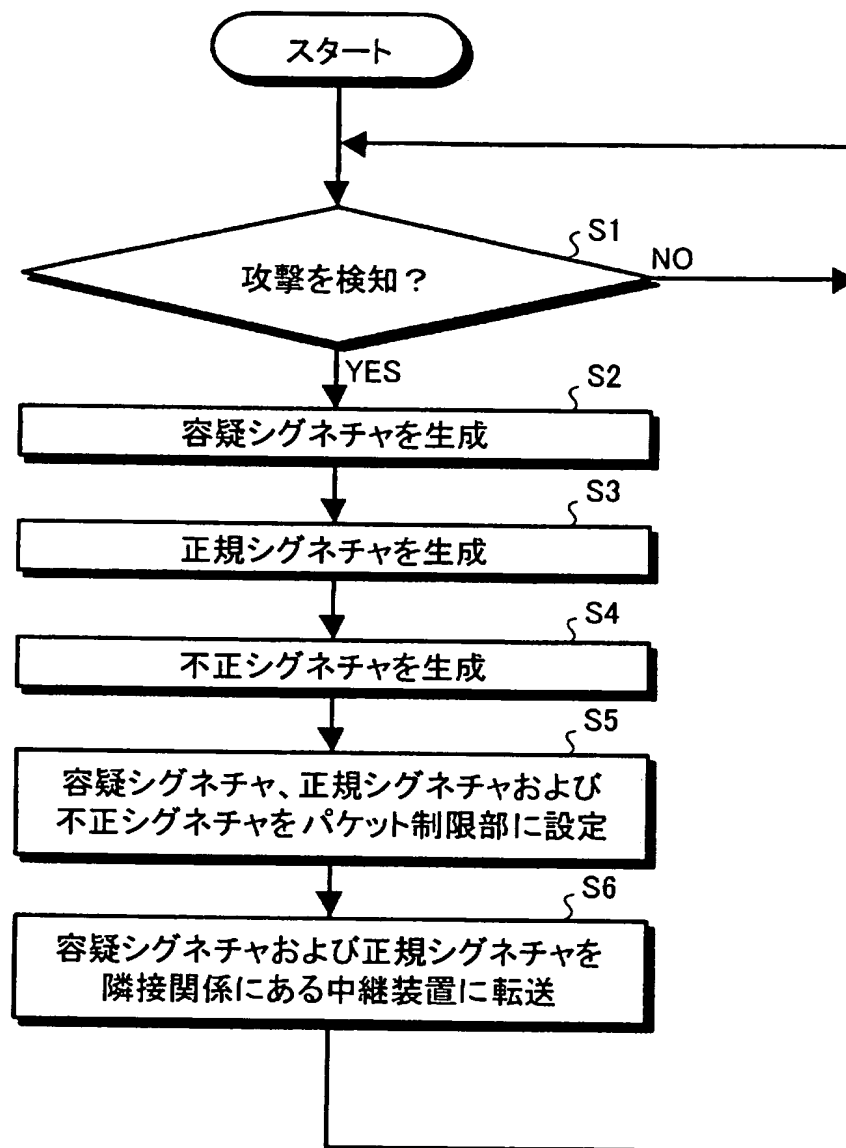
【図 5】

	不正条件
1	500kbps以上のパケットが30秒以上連続送信されている
2	300kbps以上のICMP/Echo Replyパケットが15秒以上連続送信されている
3	300kbps以上のフラグメントパケットが15秒以上連続送信されている

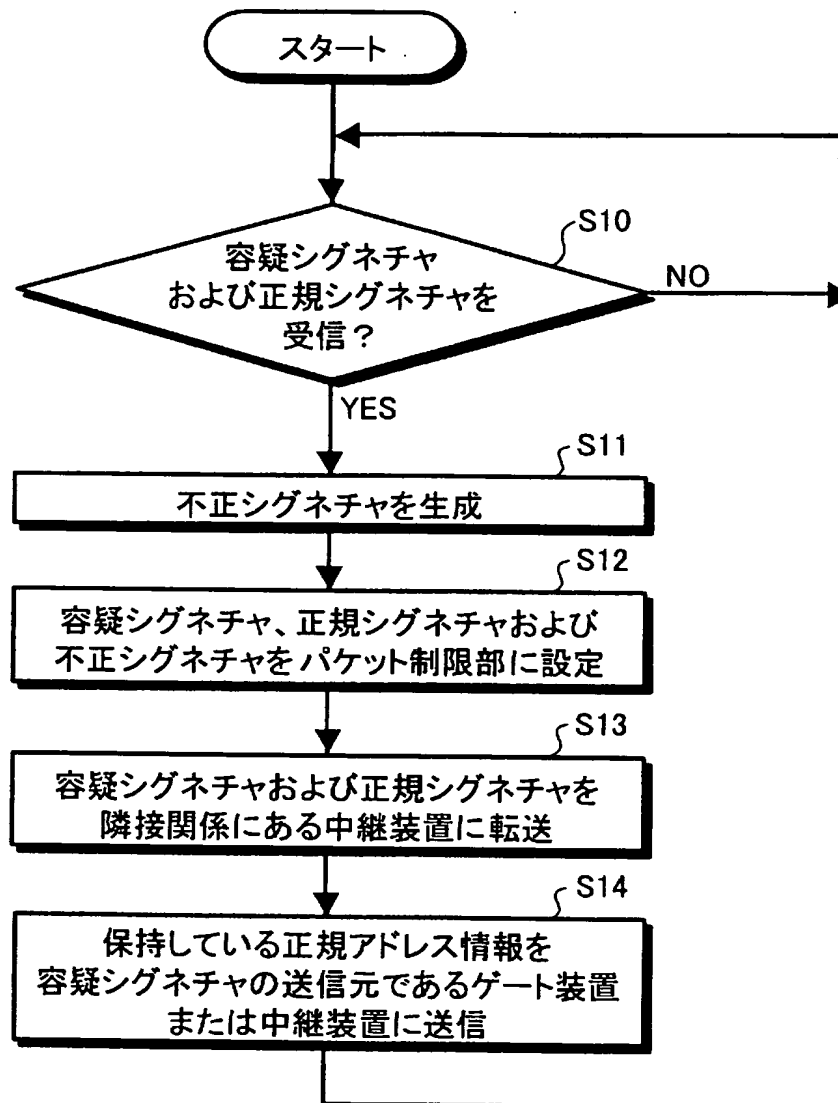
【図 6】



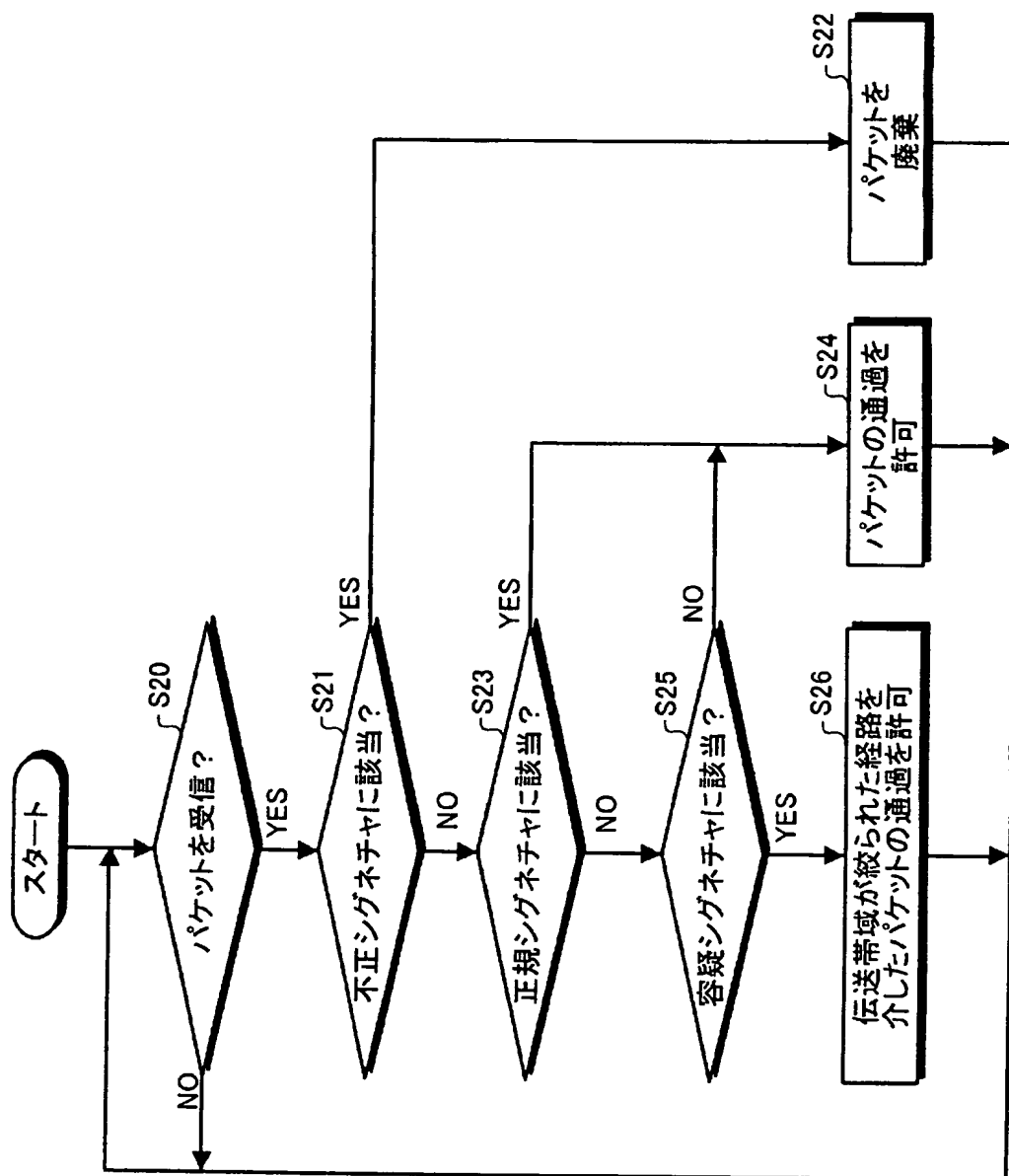
【図 7】



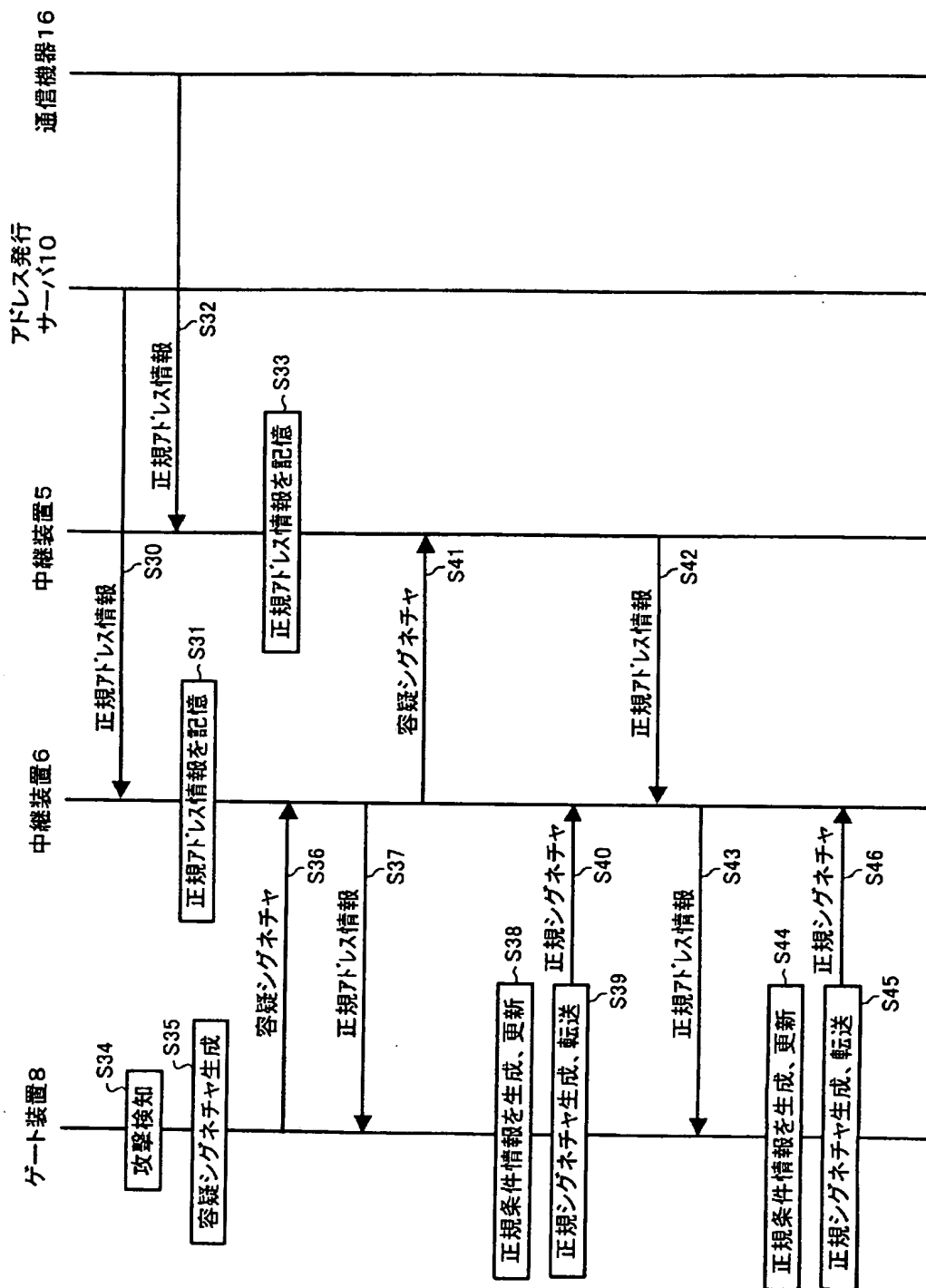
【図 8】



【図 9】



【図10】



【書類名】要約書

【要約】

【課題】防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することを課題とする。

【解決手段】ネットワーク2上に所在する正当な装置（アドレス発行サーバ10）により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置8が取得し、取得した正規アドレス情報に基づいてゲート装置8が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器7へ攻撃をおこなうパケットの通過を制限する。

【選択図】

図1

出願人履歴

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号
日本電信電話株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.